Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Tuesday, December 27, 2005

A tamper evidence protocol from China

In "The Playdough Protocols" I described how ancient Sumerians used tamper evidence both in the form of physical seals and in the form of tamper evident numbers, in particular checksums. These are forerunners both of modern plastic sealing (used for evidence bags, in banking to store and transport cash and other valuables, to protect food from tampering, and so on) and modern cryptographic hash functions, whereby one can detect whether digital content has been altered.

Daniel Nagy has uncovered a more particular connection between ancient auditing techniques and modern cryptography. He writes how Chinese merchants, at least as far back as the 3rd century A.D., used remainders of division by prime numbers instead of checksums to ensure that nothing had been stolen from storage or cargo. The security of the Chinese system was based on what we still call the Chinese Remainder Theorem. The theorem is also used in some modern cryptographic systems based on the difficulty of factoring, and in particular the RSA scheme for decryption and digital signatures.

Posted by Nick Szabo at 8:41 AM

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ► 2006 (130)
- ▼ 2005 (44)
  - ▼ December (16)
    - Robotic structures
    - Patents: the problem of gratuitous elements
    - LabCorp v. Metabolite briefs
    - The security and productivity of farms
    - A tamper evidence protocol from China
    - Secure property titles and development
    - The Justice Department vs. the United States Cons...
    - New Zealander challenges Amazon one-click patent
    - New book -- The Origins of Value
    - Copyright v. the blogosphere?
    - RIM asks Supreme Court to hear BlackBerry case
    - U.S. patent reform dead for this year
    - Another proposed amendment
    - What three constitutional amendments would you lik...

Relationship rights and the United States Supreme ...

The negative rights debate continues

► November (5)

► October (23)

Simple theme. Powered by Blogger.